boxboat
an IBM Company

CASE STUDY

How a Multinational Financial Services Firm Secured their Software Supply Chain with In-toto and SPIRE

A large multinational financial services firm with over 200,000 employees, $25 trillion in assets under custody, and operations in over 150 countries approached BoxBoat for help improving its security posture.

SUMMARY

In-toto is open source software that:
- **Cryptographically signs artifacts**
- **Provides artifact provenance**

Zero Trust Architecture tools
- **SPIFFE**
- **SPIRE**

The Solarwinds scare

Like many others in the financial services industry, this firm was alarmed by the 2020 Solarwinds hack. As their internal IT security team started mapping how all the potential vulnerabilities could impact their organization, particularly those related to securing their software supply chain, they realized that the resulting diagram was incredibly complex.

"They started saying, what could possibly break this one?" said Brandon Mitchell, Solutions Architect at BoxBoat. "How could an attacker get into this piece?" In the end, the team thought they had an idea of everything that needed to be fixed — a good first start, but also sobering — these were production systems, and implementing the fixes as quickly as possible was essential.

The internal IT Security team was planning to rely on tools such as in-toto and SPIRE to protect their software supply chain. However, their team didn't have experience with those tools. They reached out to BoxBoat because the BoxBoat team has experience working on similar projects with other

companies, as well experience with both open source projects, especially in-toto. BoxBoat has its own fork of in-toto and has been very involved in the project, so BoxBoat was clearly the right partner to use in-toto and SPIRE together to secure the bank's software supply chain.

A sophisticated team

The internal security team at the financial institution is very sophisticated and would probably have been able to implement a secure solution themselves given enough time. However, it would undoubtedly have taken them longer, and the lack of experience would have increased the risk of the implementation.

And when it comes to security, timing is important. At the time the financial institution engaged with BoxBoat, there was already a well-publicized hack that had happened, and the institution was worried that it could be targeted at any time.

Even though the internal team had the skill to both plan and execute on its own, doing so would have left the institution vulnerable for too long.

The goal

Security has a bad reputation among developers for slowing things down — and it's true that security checks, particularly manual checks, can both slow the release process down and reduce the overall security of the application. The goal BoxBoat is working towards with the financial institution is a system where developers can just hit commit and not have to worry about security at all. Once code is committed, the system will automatically look at all the other upstream resources and verify that they can all be trusted. Then that will be ingested into the environment and run, with the code that was committed, through a full build pipeline. The entire process is completely automated, so the financial institution won't have to rely on individual developers to ensure that every bit of code is properly tested and secured before being put into production.

Once the automation has run, the resulting artifact will be signed and verified and can be safely deployed to the production infrastructure.

Everyone — developer, security team, CISO — can be confident that the code the developer committed is secure and that nothing in the testing process pulled in something malicious from outside.

The solution

To achieve the financial institution's goal of hardening their software supply chain, BoxBoat designed and implemented multiple security controls to protect the build process. In-toto was leveraged to cryptographically sign software artifacts created during each step of the build process. It also provides artifact provenance – this ensures that the software artifact was built according to the proper specifications and controls. In-toto was directly integrated into the financial institution's existing security controls for software builds, and allows the IT security team to cryptographically validate that the build process is secure.

In addition, BoxBoat implemented a Zero Trust Architecture using tools such as SPIFFE and SPIRE. These tools, combined with other open source technologies, allow the financial institution to validate artifact signatures, metadata, and provenance before they are deployed to production. The tools ensure that the correct software is running in the correct environment with the correct permissions, and that the build process has not been intercepted by malicious actors.

Protecting end users

As important as streamlining the development process is, the ultimate beneficiary of tighter security practices are end users. Protecting end user information, financial information, and protecting against data loss and leaks are all extremely important in the context of a bank. Not only would a breach be potentially devastating for end users, it could also be extremely expensive in the face of regulations.

Working with BoxBoat to ensure the software supply chain is as secure as possible at all times protects not just the financial institution's interests, but also end users' financial data.